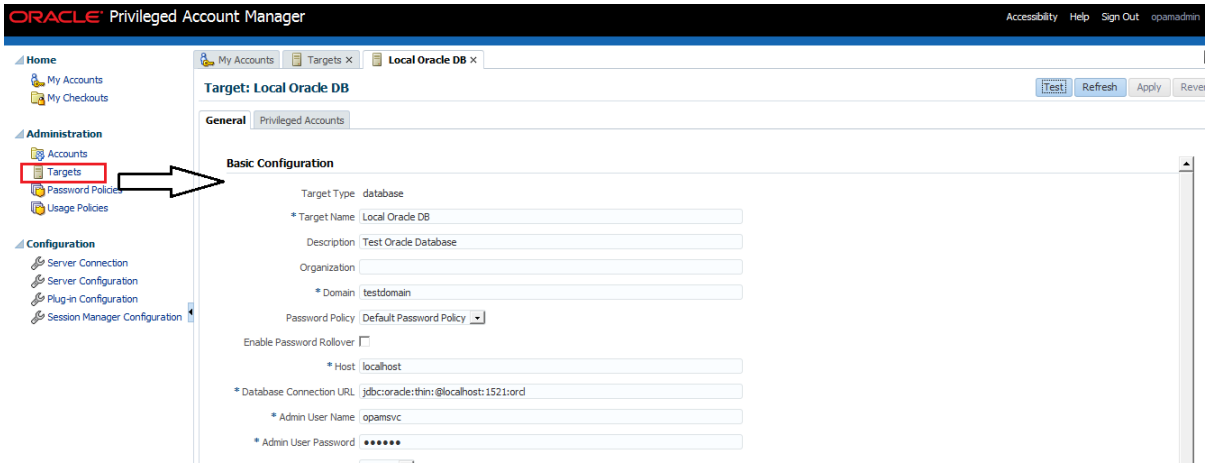
# How to manage Privileged Accounts on Targets via OPAM?

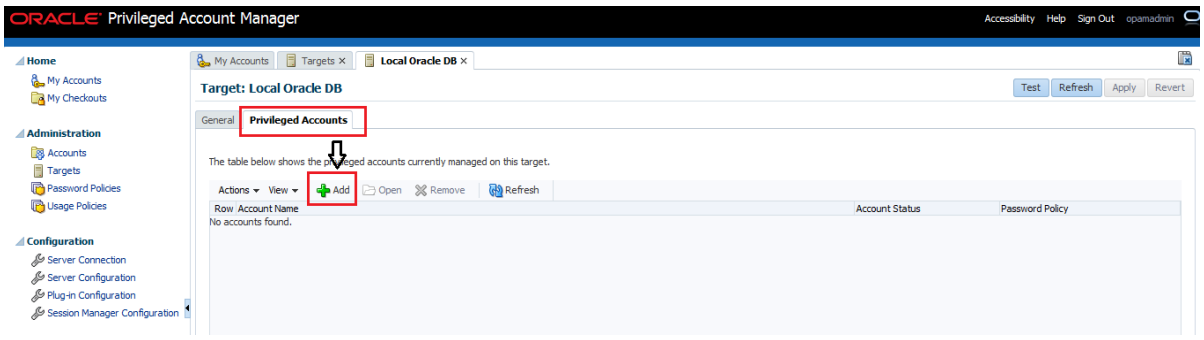
***Privilege account managed is the CORE OPAM functionality.***

This document describes it via a simple use case w.r.t managing a privileged account on an Oracle DB

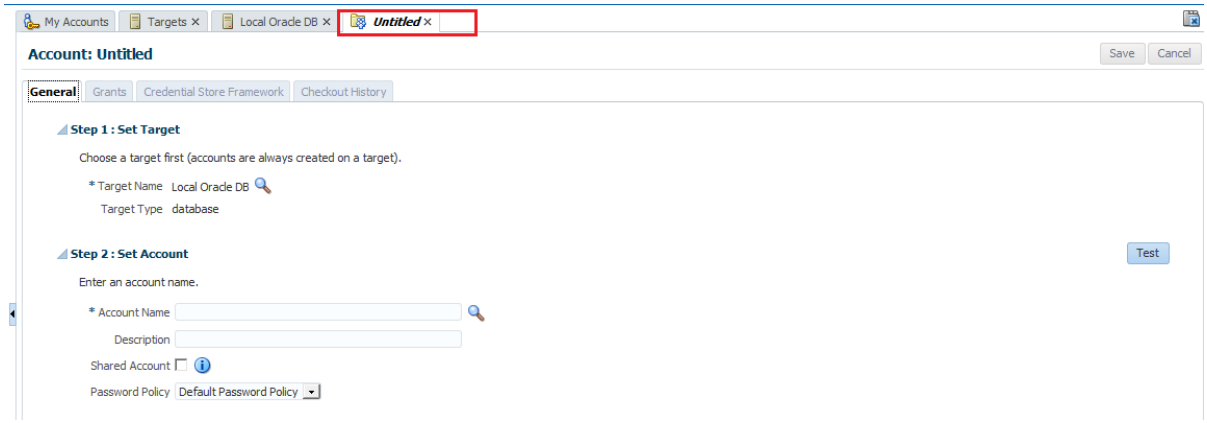
1. **Register the privileged account in OPAM**

Open the Target System on which you want to manage the privilege account

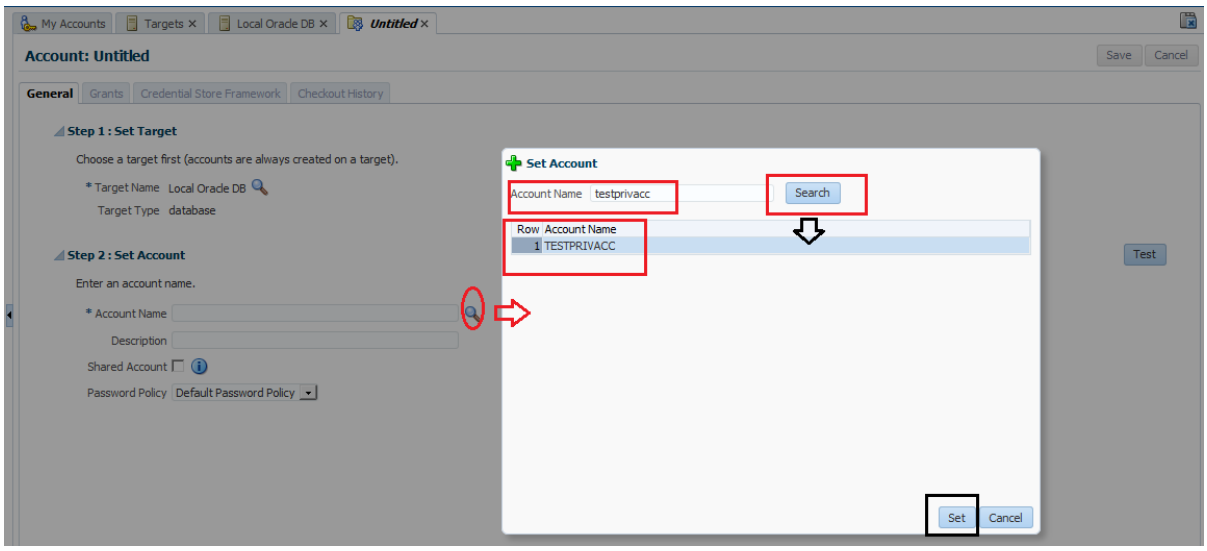


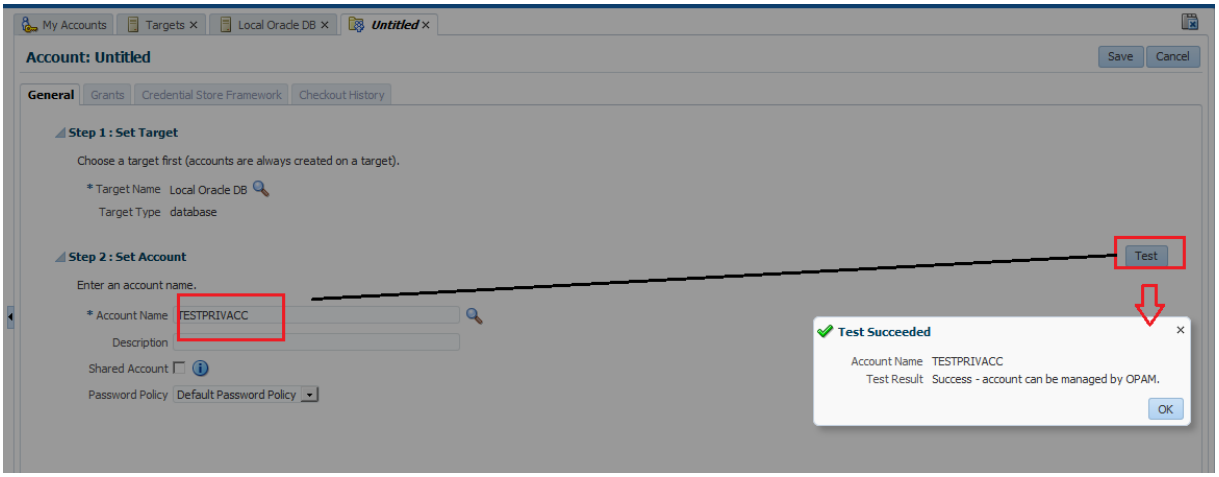




A new tab opens

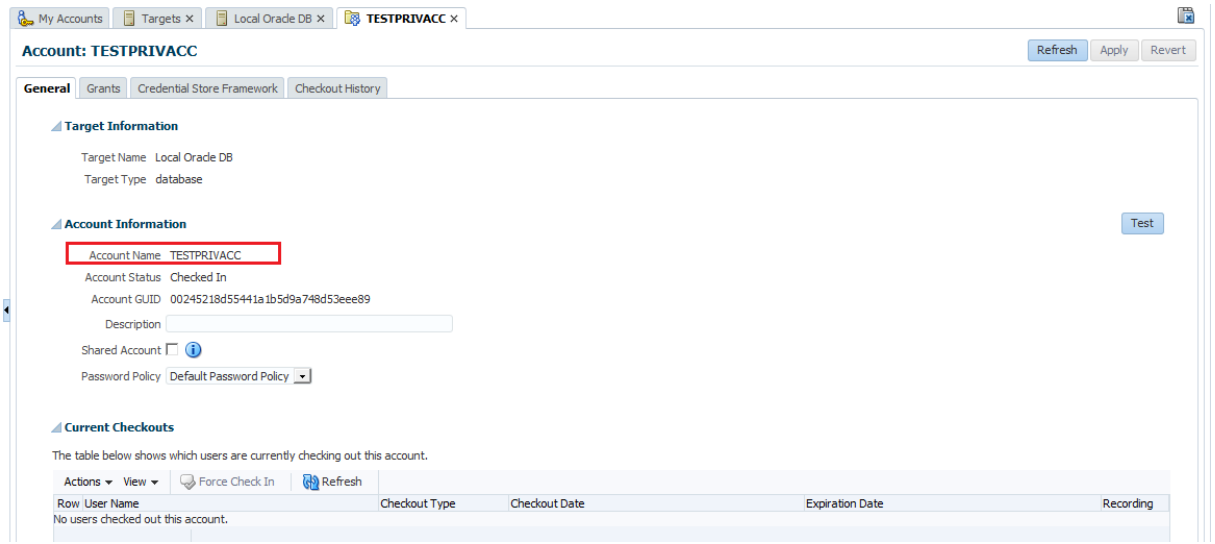



Add an account - you can search for the accounts directly from the OPAM console



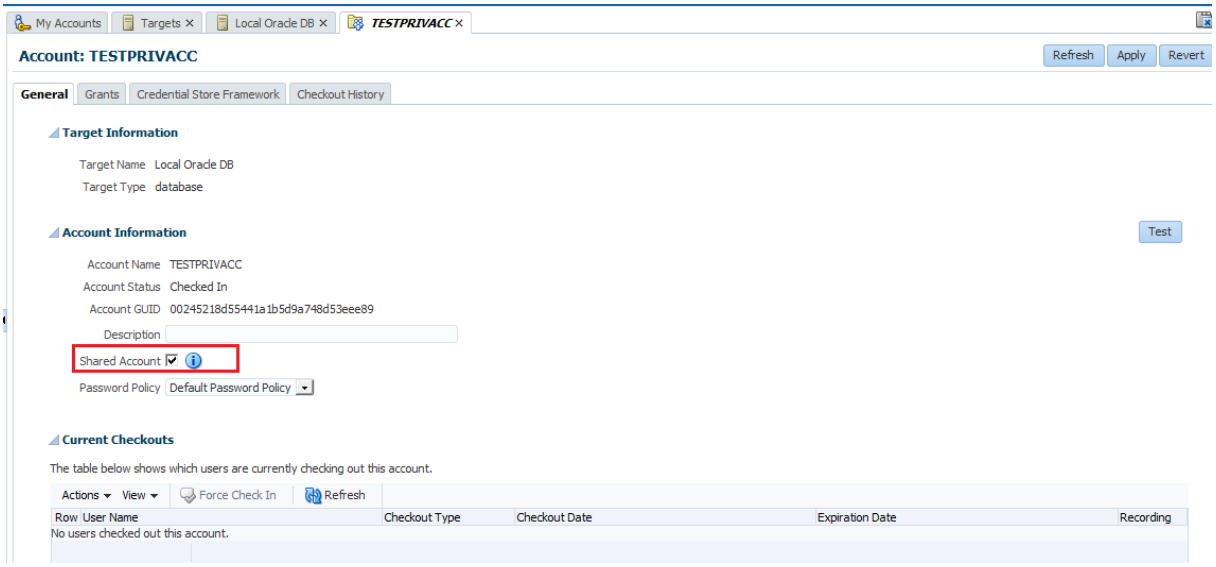



Click Save to finalize



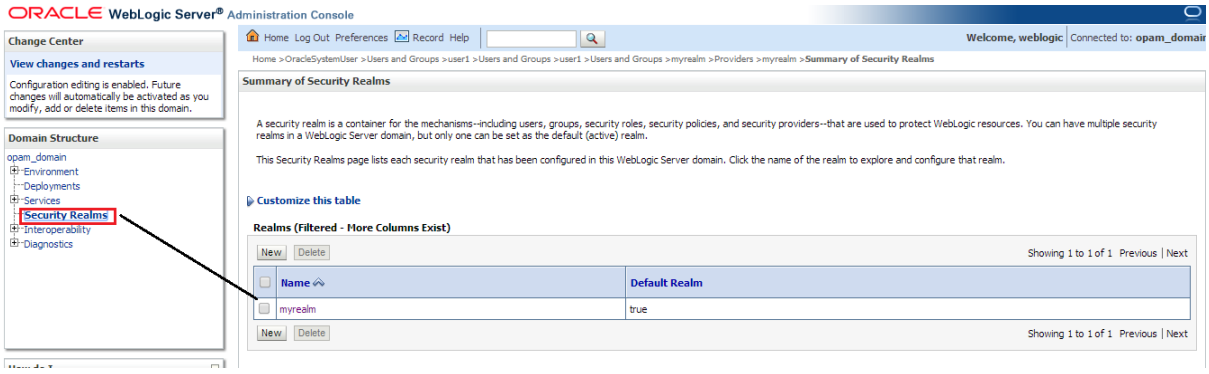

**Note on Shared Accounts**

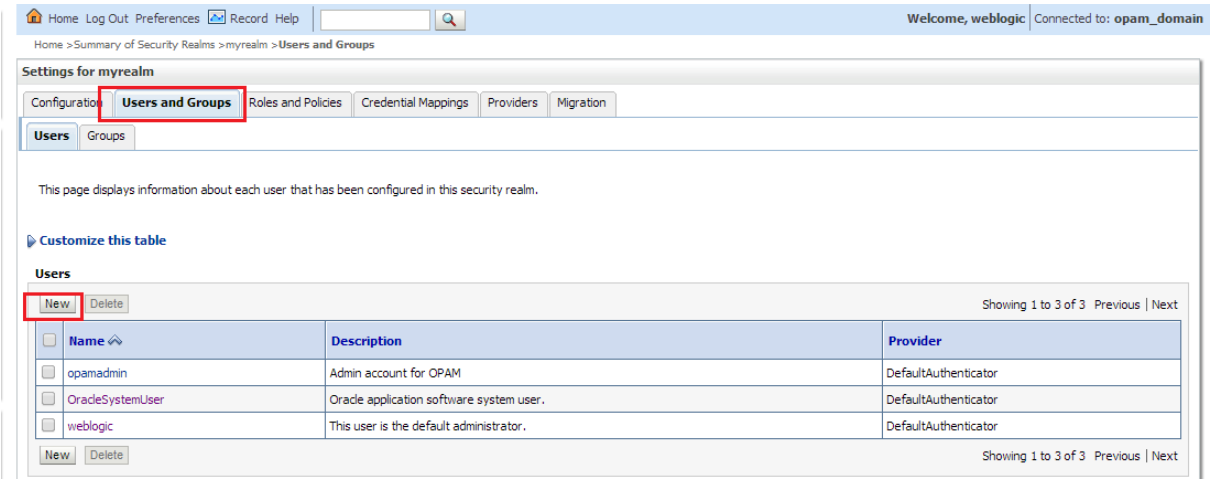
*If you enable shared accounts for a particular account, multiple users can check them out at once - NOT RECOMMENDED*

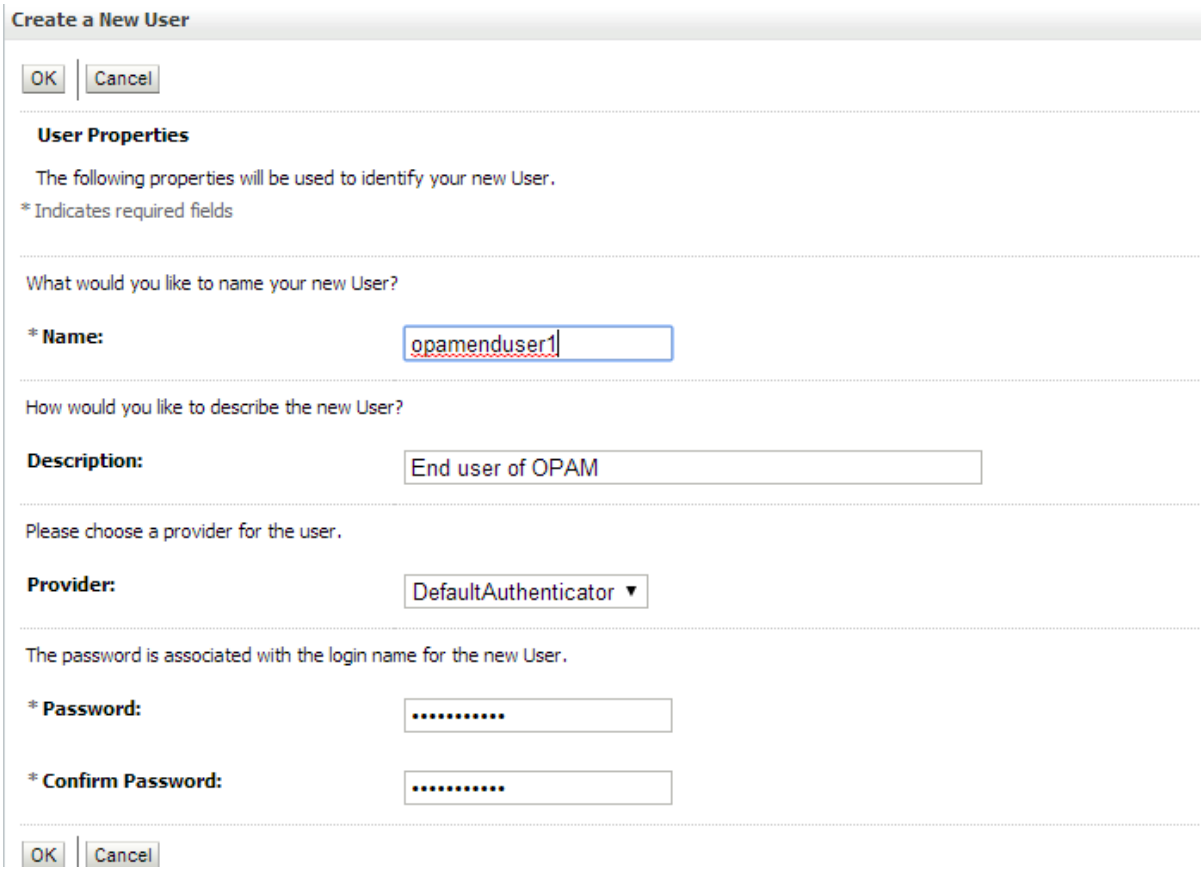


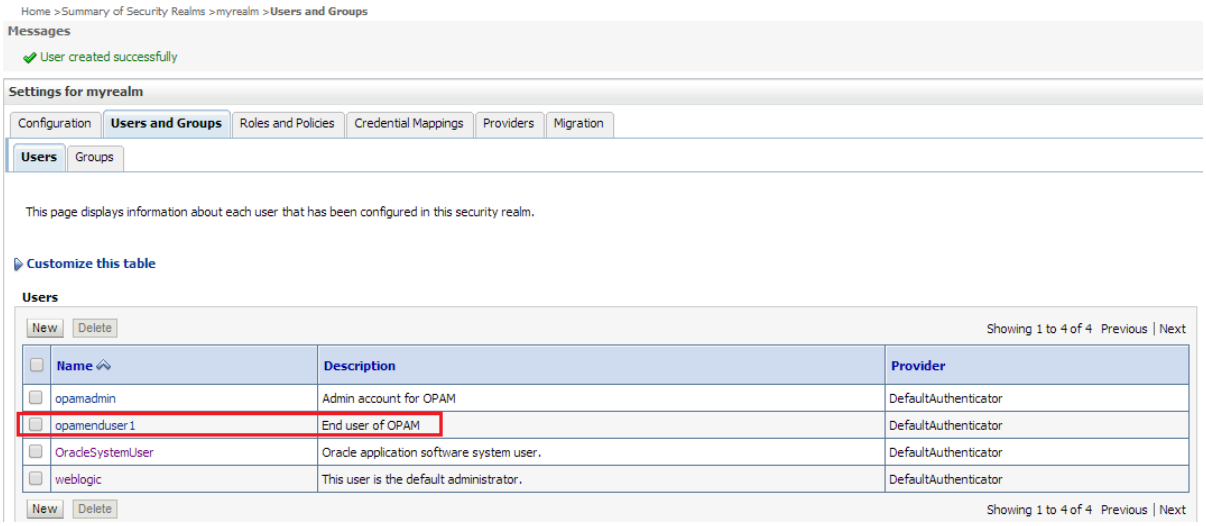

2. Ok, so we now have a privileged account. **Who is going to use this account? Let's configure a test user and grant this account to him**

Log into Weblogic Admin console and create the user first - this will done in the embedded Weblogic LDAP which is being used as the Identity Store for OPAM



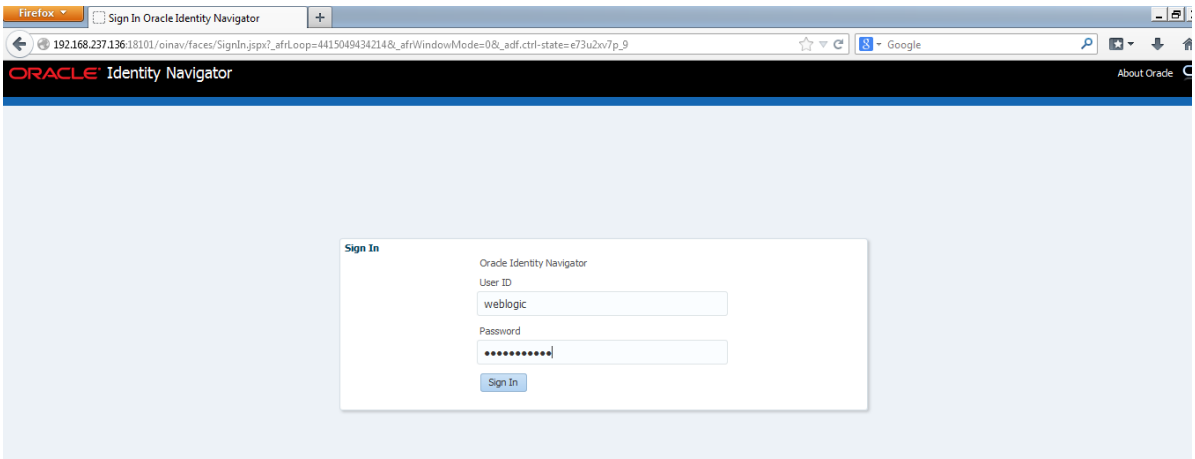

Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: opam_domain
Home >Summary of Security Realms >myrealm >Users and Groups
Settings for myrealm
Configuration
Users and Groups
Roles and Policies
Credential Mappings
Providers
Migration
Users
Groups
This page displays information about each user that has been configured in this security realm.
Customize this table
Users
New
Delete
Showing 1 to 3 of 3 Previous | Next
Name
Description
Provider
opamadmin
Admin account for OPAM
DefaultAuthenticator
OracleSystemUser
Oracle application software system user.
DefaultAuthenticator
weblogic
This user is the default administrator.
DefaultAuthenticator
New
Delete
Showing 1 to 3 of 3 Previous | Next

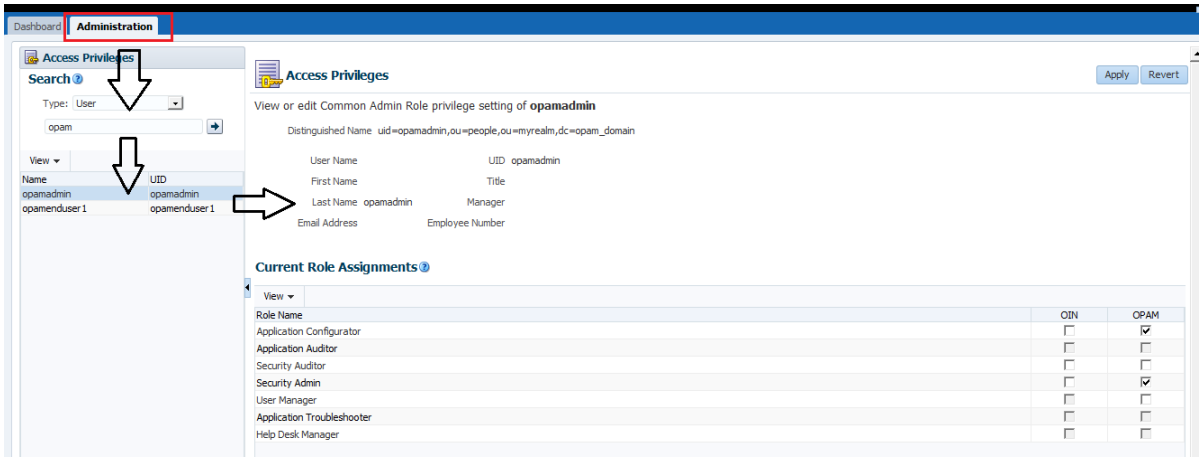

Create a New User
OK
Cancel
User Properties
The following properties will be used to identify your new User.
* Indicates required fields
What would you like to name your new User?
* Name:
opamenduser1
How would you like to describe the new User?
Description:
End user of OPAM
Please choose a provider for the user.
Provider:
DefaultAuthenticator
The password is associated with the login name for the new User.
* Password:
* Confirm Password:
OK
Cancel



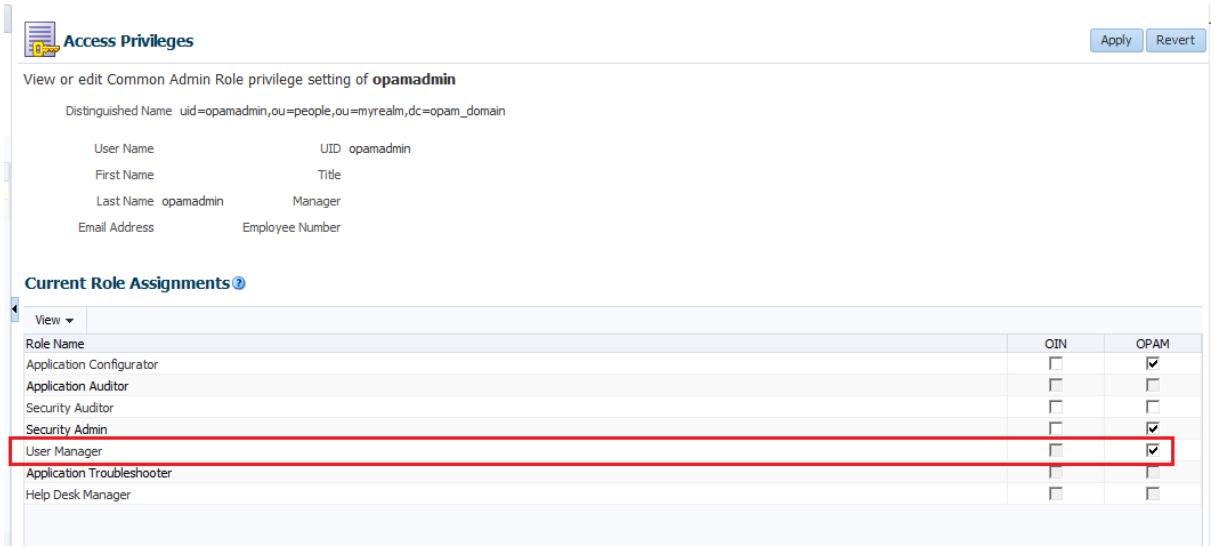

To Add grantees for an account, the OPAM user has to have the User Manager Admin Role

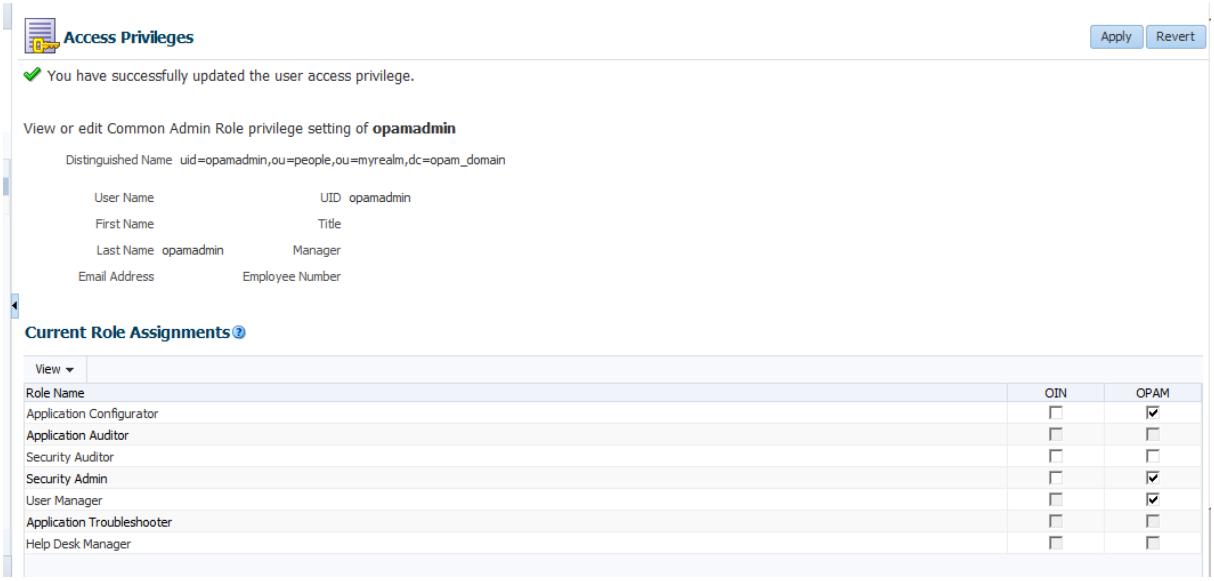
Log into OIN



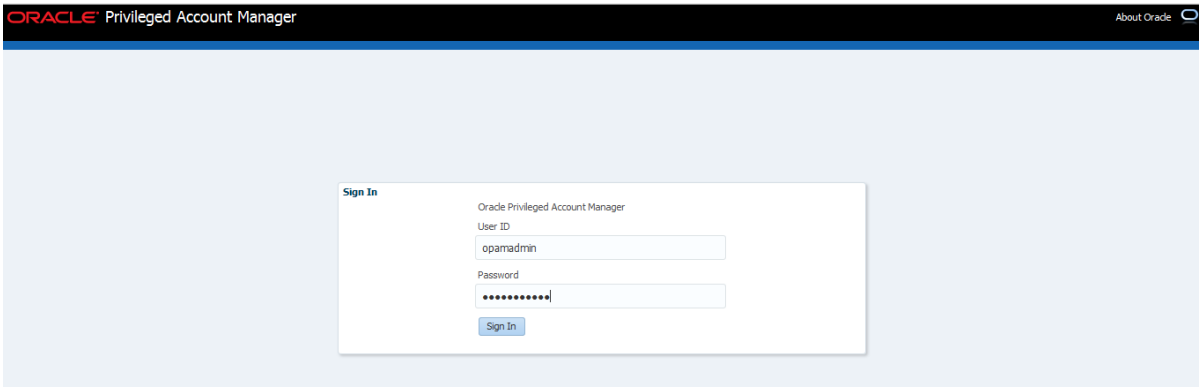



Choose your desired roles - in this case User Manager

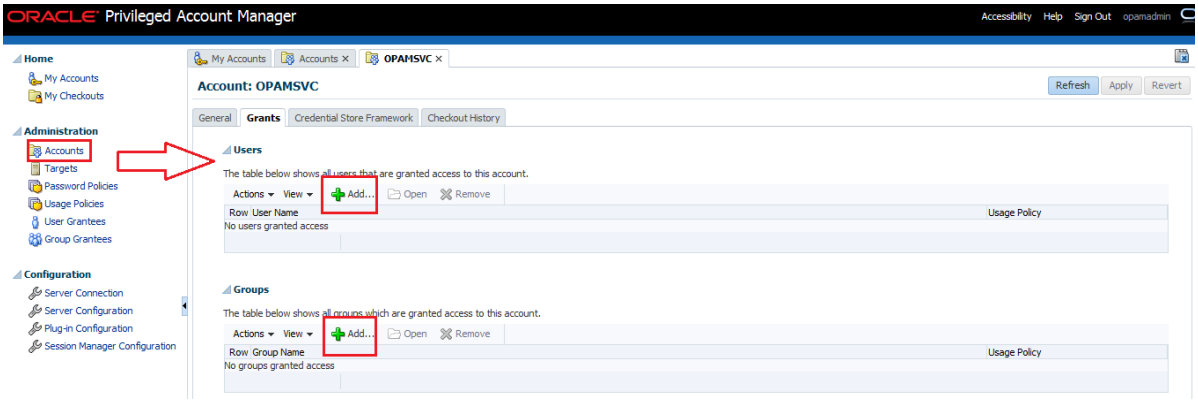




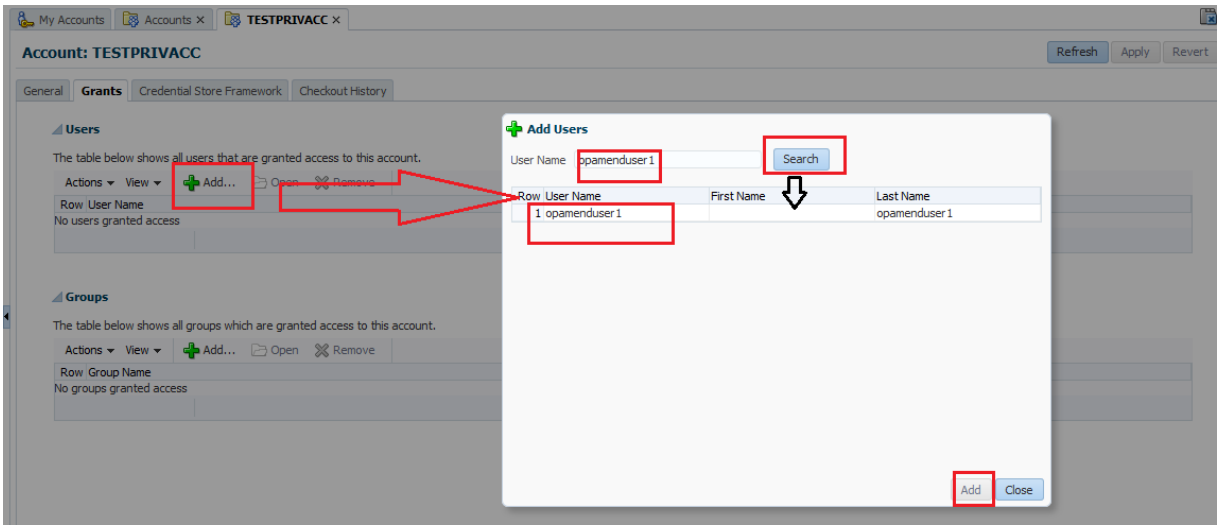

Log into OPAM now

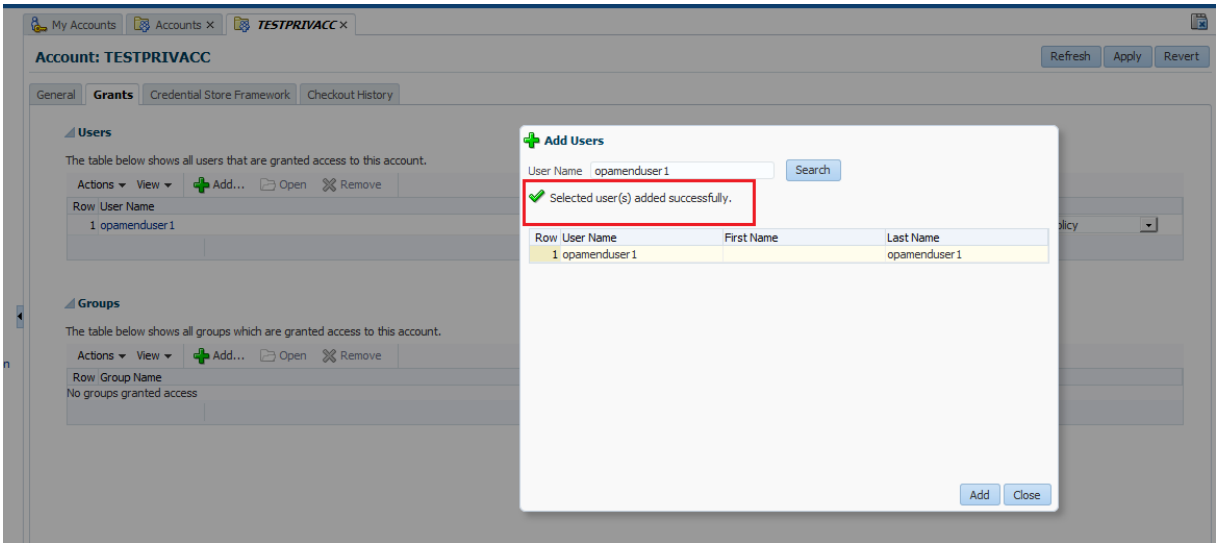



The Add option is available as a result of the User Manager Admin Role grant which we executed above

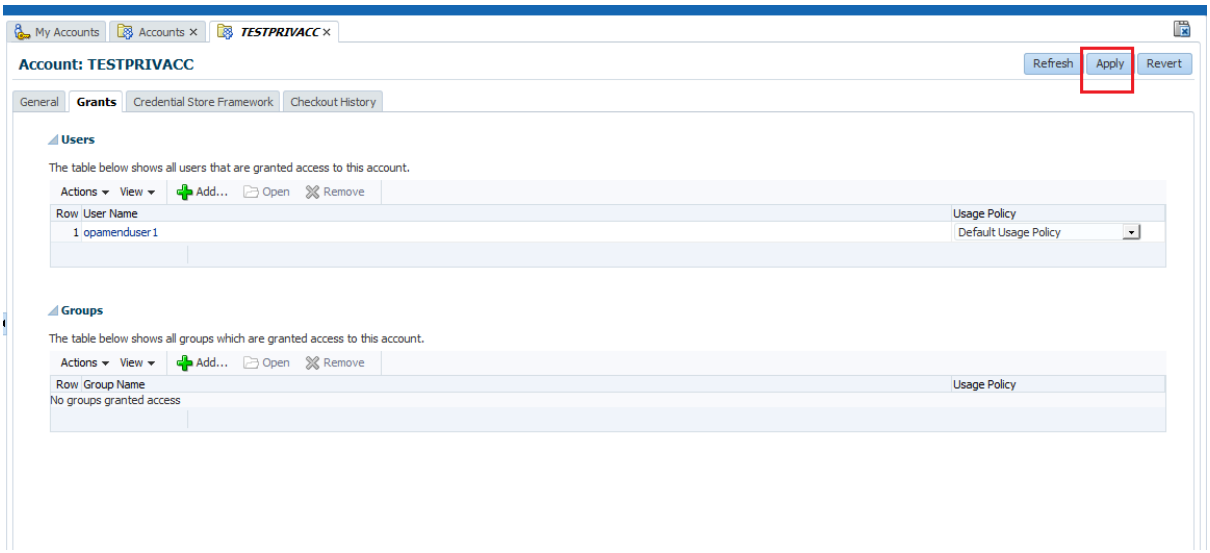


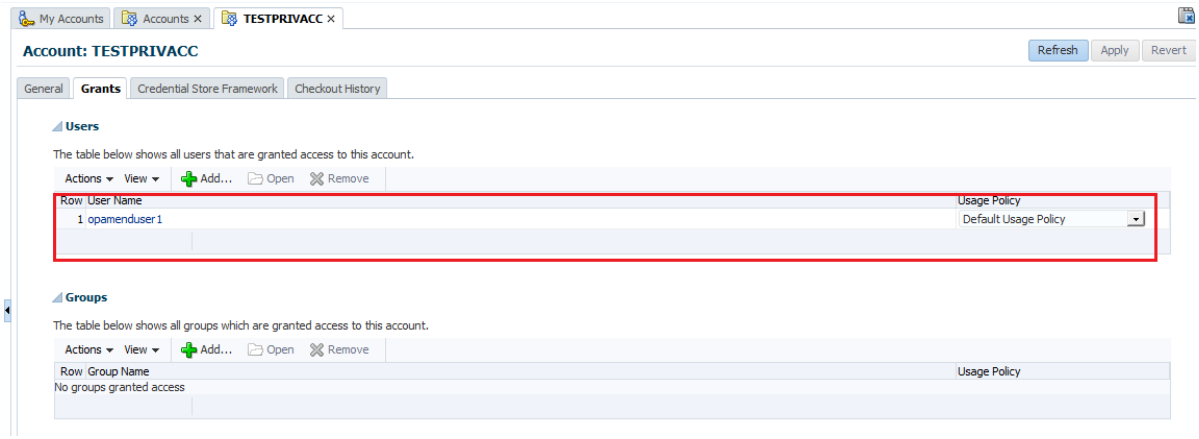

Proceed to grant users to accounts





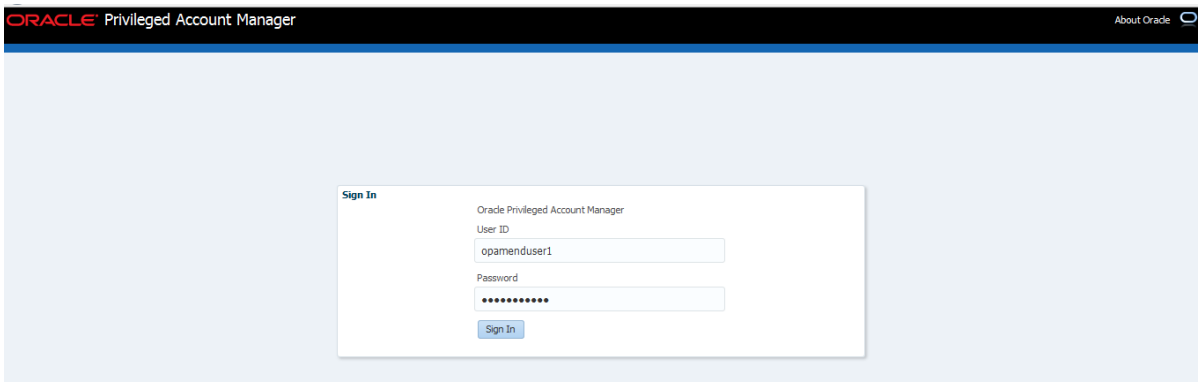

Apply to save



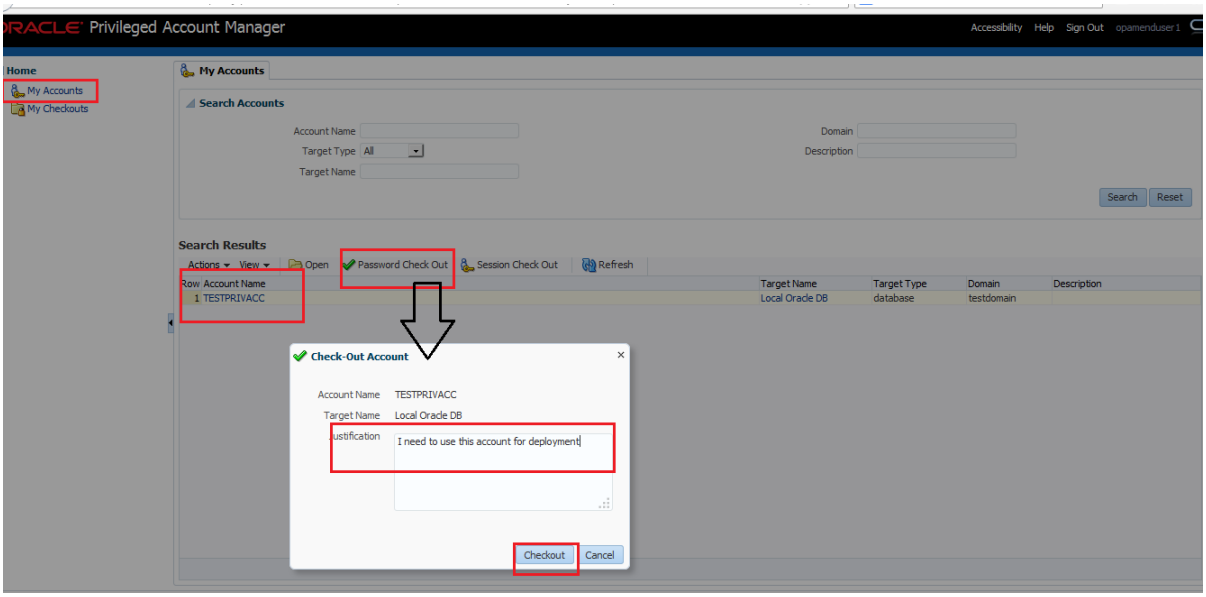



3. Now we have a privileged account registered into OPAM and it has also been granted to an end user for him to be able to use this account. **Let's see how OPAM lets an end user leverage this facility in a secure manner**

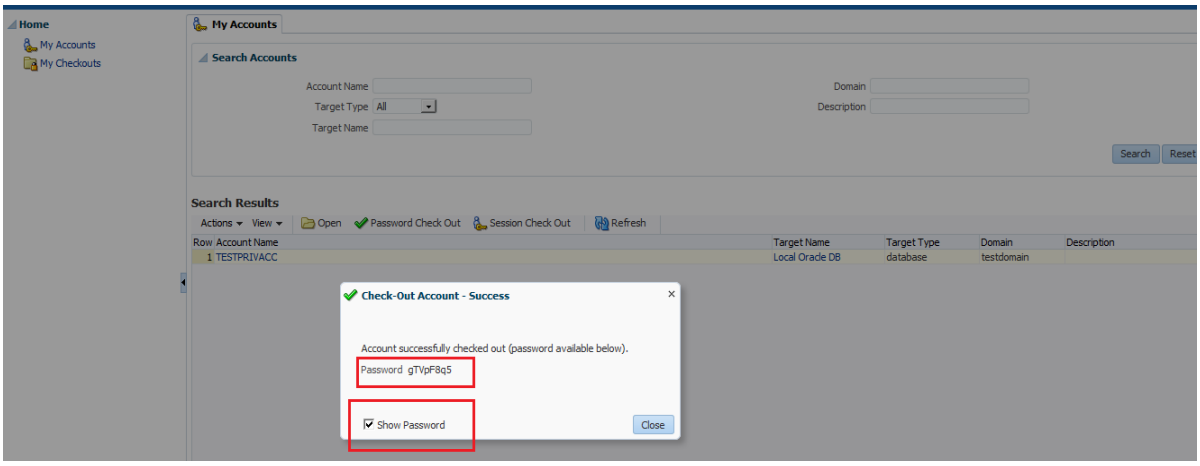
Log into OPAM using end user credentials (we created this in the above step)



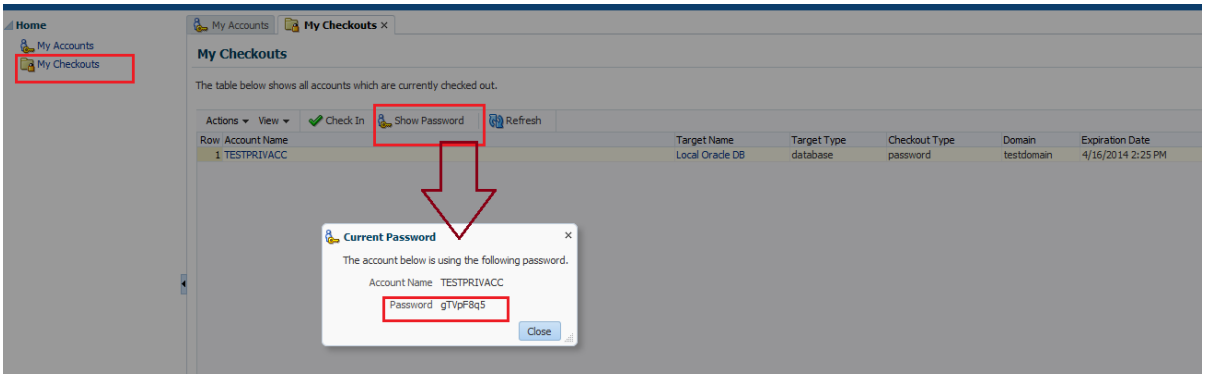

Check out the account for usage



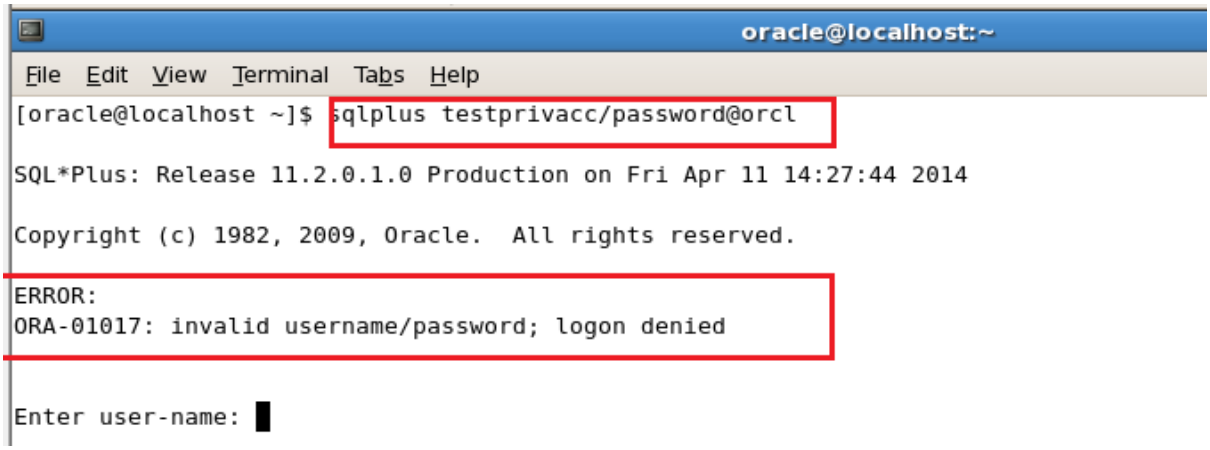

As soon as you check out an account, it's password automatically changes and is reset to a random password and is available to the end user




The information is also available under My Checkouts section




If we try to login to the account in the actual Oracle Database using the old password, it will fail



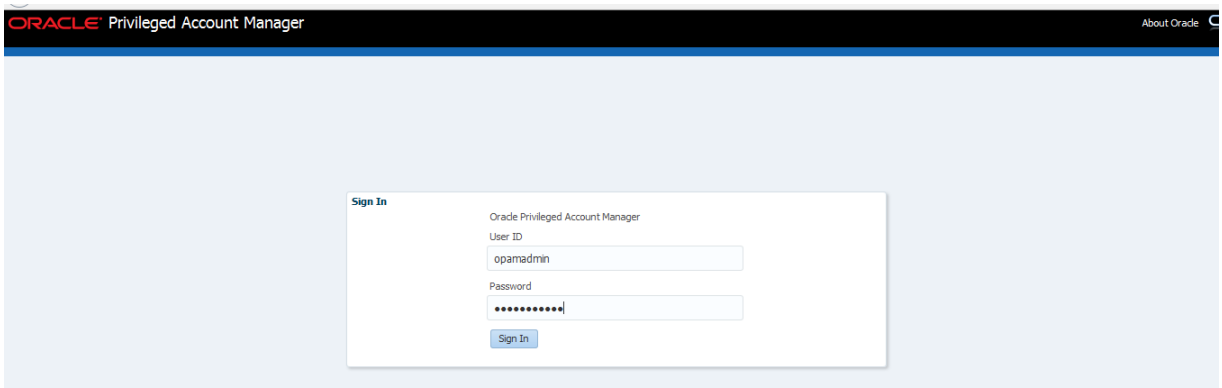

Try to login using the password provided by OPAM (see above)

```
oracle@localhost:~
File  Edit  View  Terminal  Tabs  Help
[oracle@localhost ~]$ sqlplus testprivacc/gTVpF8q5@orcl

SQL*Plus: Release 11.2.0.1.0 Production on Fri Apr 11 15:00:25 2014

Copyright (c) 1982, 2009, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL>
```

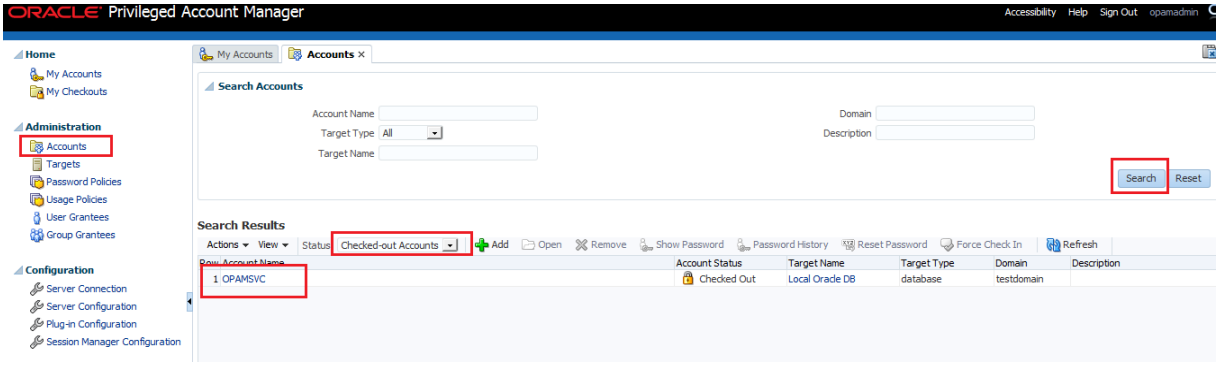
4. Alright. The end user is now using the password to log into his Oracle DB account to perform his activities

**How can this be monitored?**

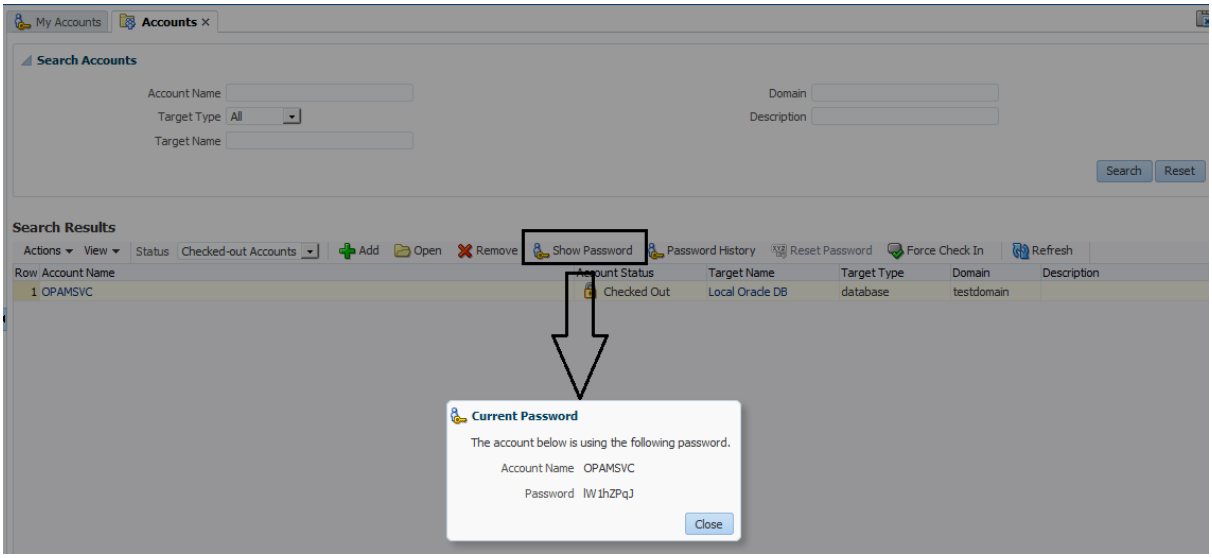
Login as Admin user into OPAM



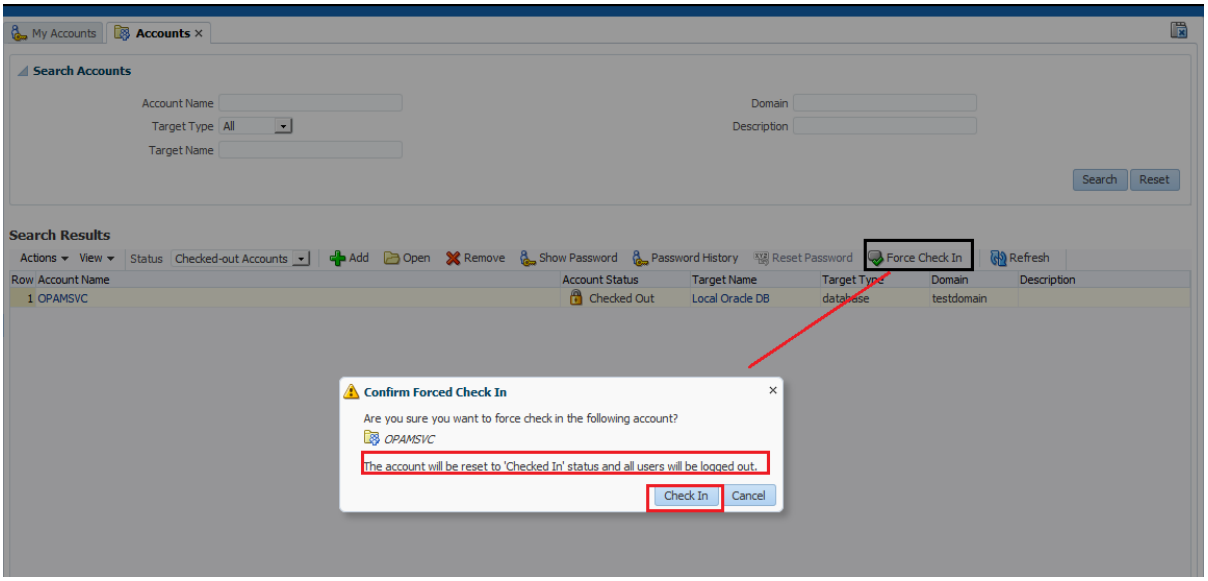

Filter by Checked Out Accounts




Admin can see the current password



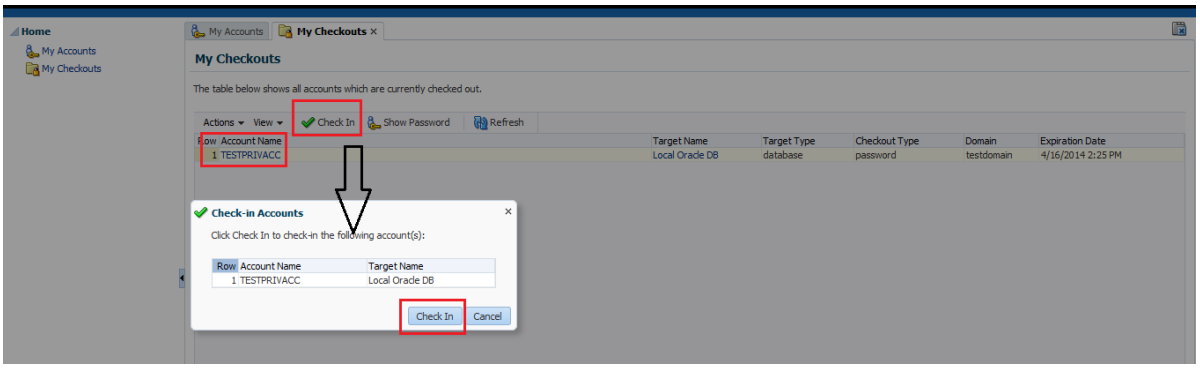

Admin can forcibly check in the password - this will RESET the password and the end user will be unable to use the same



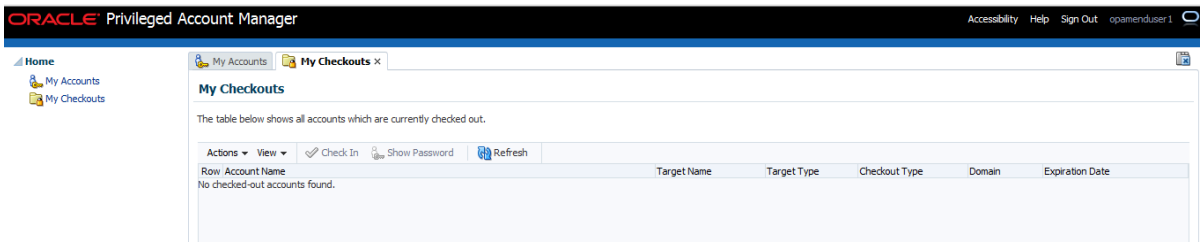

5. **Now, the end user has finished his work and wants to check in the account**

Checking the account in will automatically reset its password

Log into OPAM as an end user

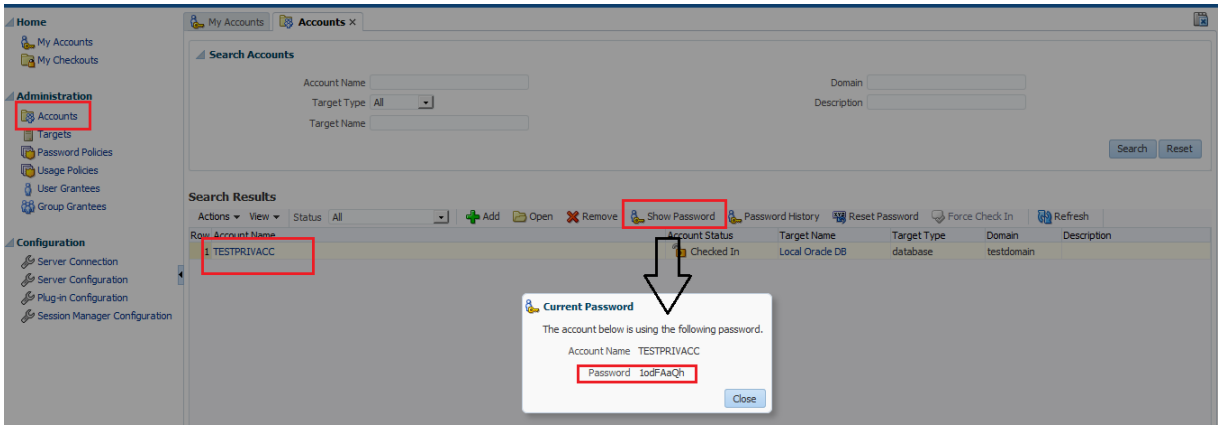



No more checked out accounts for the end user




6. **Let's confirm whether the password has actually been updated/changed after the check in**

Log in as admin user in OPAM. See the highlighted password below and the password obtained above - they are different




As expected, old password will not work anymore

```
oracle@localhost:~
File  Edit  View  Terminal  Tabs  Help
[oracle@localhost ~]$ sqlplus testprivacc/gTVpF8q5@orcl

SQL*Plus: Release 11.2.0.1.0 Production on Fri Apr 11 15:20:22 2014

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

ERROR:
ORA-01017: invalid username/password; logon denied


Enter user-name:
```